# CHAPTER 2

# SYSTEMS ENGINEERING AND SYSTEMS SAFETY

## 2-1. General systems considerations

Requirements are presented in this manual for the design of optimally reliable, safe, self-contained C4ISR utility systems and for the design of conventional electrical power and other utility services. These utility systems shall be capable of supplying services continually to the C4ISR installation site during any natural or man-made disruption in commercial services. Off-site power facilities are assumed to be adequate to supply peak power demands, but are not assumed to be uninterruptible. Potential threats include physical attacks; biological, chemical, and radiological warfare; and close-in and high-altitude nuclear blasts.

## 2-2. Program elements

The essential elements of a system's engineering program are described below. They shall be considered in light of the organization's mission and function; the availability of existing natural and manmade resources and the security necessary for a new or existing facility.

a. Reliability, availability, and maintainability (RAM) requirements shall be implemented during design by the design agency to maximize the availability of the C4ISR utility systems.

b. Human factors engineering (HFE) activities will ensure that reliability, availability, and safety of the C4ISR power system are not degraded through human activities during operation or maintenance. The design agency shall accomplish the HFE program requirements through the use of established standard HFE design criteria and practices based on MIL-STD-1472, Human Engineering Design Criteria for Military Systems, Equipment, and Facilities.

c. The C4ISR power system safety program shall ensure that the design incorporates, within program restraints, the highest attainable level of inherent safety. It shall eliminate or reduce the probability of events that can cause injury or death to personnel, or damage to or loss of equipment or property. For example, pipes, lines, and tanks shall be placed away from high-traffic areas. Safety documentation shall be provided for safety items that require designation or may cause action during subsequent program phases. The design agency system safety program shall be based on a philosophy that the most effective actions to control potential hazards are those taken early in the design process.

(1) When hazards cannot be controlled by design measures, including safety and warning devices, special operating procedures shall be developed and documented. The safety program shall provide support to the systems engineering (SE) program and shall ensure that the applicable requirements of MIL-STD-882, System Safety Program Requirements, are met.

(2) The systems safety program shall define and address the system safety analyses that shall be performed during development of design. During the early design phase, an analysis that identifies conditions that may cause injury or death to personnel and damage or loss to equipment and property shall be performed. Prior to the final safety design review, the design agency shall perform a second systems safety analysis to determine adherence of the design to all required safety standards and criteria, and to ensure avoidance or reduction of identified hazards. Operating and maintenance procedures shall also be reviewed for compliance with all required safety standards and criteria.

(3) The systems safety program shall include procedures to ensure that safety hazards identified by the systems safety analyses are eliminated or reduced to acceptable levels of risk, and that those actions taken are fully documented.

(4) The design agency shall prepare specific safety program documentation. This documentation shall include, but not be limited to, safety analysis reports and the final systems safety report.

d. The design agency shall develop a consolidated systems test program that covers all phases of testing, develops confidence in the system, and provides means for interim and final acceptance of equipment and systems. The design agency shall minimize cost through elimination of testing duplication and by maximizing the collection of data for each test. Successful completion of these tests shall be accomplished prior to final acceptance.

e. The design agency shall develop and implement a standardization program to minimize equipment and component stockage. Redundant systems shall be of the same design.

f. The configuration management (CM) program shall maintain effective control over design from criteria development through design, construction, and installation of the equipment. A government configuration control procedure shall be developed by the design agency for use in the C4ISR utility systems configuration control program.

g. Operations and maintenance (O&M) planning will be done by the design agency and shall identify and recommend essential items of the program during the design phase. A reliability centered maintenance (RCM) program should be implemented to identify single point failures and identify the critical systems. Basic elements of the program are as follows.

(1) As part of the SE database, data requirements shall be identified for preparation of O&M manuals. Systems functional descriptions shall be developed. Requirements shall be developed for data collection, including repair parts list, calibration requirements, special tools and test equipment, repair parts stockage level, and shelf life data. Repair parts list, repair parts stockage level, test equipment, and test frequency shall be provided for the using government agency.

(2) Systems and equipment of high complexity or peculiarity shall be identified, and special training for personnel who operate and maintain such systems and equipment shall be identified.

(3) The design agency shall identify those items critical to accuracy and repeatability, and shall recommend calibration requirements. Unique calibration requirements and procedures shall be provided whenever necessary.

(4) Systems test and checkout requirements to be performed following major maintenance activities shall be developed during design to ensure safe and normal operation of the system.

## 2-3. Systems engineering database

The systems engineering database (SEDB) shall serve all data needs for the system from functional equipment development to final design. The design agency shall develop the formats for data input and output. Cross-references shall be made between required data elements and required deliverable documentation.

## 2-4. Reliability and availability (R/A)

The R/A design goal for each of the C4ISR utility systems subsystems shall be 0.999999 (approximately 31 seconds of downtime per year) unless the using government agency determines that a greater frequency of mission outages is acceptable. The C4ISR utility systems design shall be evaluated by use of standard R/A analysis techniques to ascertain if the subsystems and mission goals have been met.

## 2-5. Life-cycle cost analysis

A life-cycle cost analysis (LCCA) shall be performed on all viable alternatives to determine the most cost-effective prime mover, auxiliaries, and supporting systems for the generator set. This analysis shall be performed in accordance with the appropriate service regulations. As a minimum, an LCCA shall be performed for the on-site mode of operation.

## 2-6. Operational control concept

All functions required to supply power to the C4ISR technical facilities shall be under the control of on-site personnel. At sites with a central power plant, operators shall be stationed in a continuously manned control room (CR). The location of the CR at such sites shall be established by the using government agency during the preparation of the project design criteria documents or during the design. Only a senior CR operator should be permitted to control equipment at equipment locations. The senior operator shall be provided with local-remote selector switches, push buttons, or equivalent and more convenient means of selecting between operation at the equipment or from the remote CR. The CR shall be equipped with all equipment or devices needed to permit operators to control electrically operated breakers; to start up, synchronize, and shut down generating units; and to observe the status or condition of the electrical and mechanical systems. Such equipment or devices include supervisory, telemetering, and data acquisition systems, if required; central instrumentation, monitoring, and control systems; indication and recording devices; and other equipment or devices noted in subsequent design requirements or as required by the project design criteria. All such equipment or devices shall be conveniently arranged in the CR on consoles, cabinets, or panels to facilitate rapid control operations under normal and abnormal operating conditions for all basic modes of operations.